EAI Endorsed Transactions
on Smart Cities

Review Article EAI.EU

# Blockchain Technology and Smart Cities- A Review

Shilpi[1,*], Mohd Abdul Ahad[2]

[1]Department of Computer Engineering, Jamia Millia Islamia, New Delhi-110025, India
[2]Department of Computer Science and Engineering, SEST, Jamia Hamdard, New Delhi-110062, India

## Abstract

Blockchain technology can be termed as a revolutionary innovation that has transformed the manner of data sharing by making it more secure and immutable. The existence of a mutual trust model which includes every participating entity makes it a widespread adopted technology in recent years. Due to its impeccable application domains the blockchain technology is slowly becoming an essential enabling technology of modern day. Smart cities ecosystem is one such domain wherein blockchain is finding numerous application and implementation avenues. Due to the diverse nature of devices and heterogeneity of data involved in smart cities ecosystem blockchain is considered an apt technology. In this paper, the current status of "blockchain based smart cities" is discussed. The paper further systematically reviews the various existing proposals, frameworks and architectures which were developed by researchers in order to mitigate the issues and challenges in the implementation of smart cities by utilizing the blockchain innovation.

**Keywords:** Blockchain, Smart City, Security, IoT

Received on 29 January 2020, accepted on 26 March 2020, published on 27 March 2020



doi: 10.4108/eai.13-7-2018.163846

*Corresponding author. Email: july23shilpi@gmail.com

## 1. Introduction

In recent years, the economic growth and social changes have initiated the largest surge of urbanization around the globe and thus more and more individuals are moving towards urban communities. As of late the "United Nations" has anticipated that "86% of developed nations and 64% of the developing nations will be urbanized by 2050" [1]. It has been indicated that more inhabitants stay in urban areas (54%) than provincial zones (46%) and this figure will increase to 66% by 2050 [2]. In order to adapt to these emergencies, urban communities focus on current advancements with a focus to minimize costs, use assets optimally, and make increasingly reasonable and feasible urban conditions.

The widespread adoption of IoTs and remote interchanges has enabled easier interconnection of gadget networks and uniform transfer of information even from remote areas and difficult terrains. Such systems, however, are largely instrumented with open information and thus must be protected against security vulnerabilities [3-4]. In order to overcome these vulnerabilities, data dependent solutions must be created to give protection, trustworthiness, and confidentiality of information. Gartner's report gauge that 30% of keen urban community's social insurance applications will have mechanical technology and innovative machines and 10% of shrewd urban communities will utilize street lamps as the spine for a system of savvy urban communities by 2020 [5]. As of late, blockchain innovation has gained popularity in numerous fields and businesses for example horticulture, digital currency, inventory network and shrewd urban areas and so on. It is also reported that $3.1 trillion will be added to the world economy by 2030 [6].

As per "Nelson Rosario" [7], the Blockchain technology is characterized as a "distributed ledger network using public-key cryptography to cryptographically sign exchanges that are put away on a distributed ledger, with the record comprising of cryptographically connected blocks of exchanges. This cryptographically connected blocks of exchanges structure is known as a blockchain." In simple words, it is a shared dispersed record innovation that "records exchanges", "understandings", "agreements", and "deals"

[8]. Primarily created to aid digital currency, blockchain technology can further be used for a variety of information exchanges using peer to peer networks. The requirement for any central authority between different parties executing budgetary and other information exchanges have been wiped out by blockchain by utilizing a transparent, immutable and a decentralized open record. This open record is a conveyed database that is shared with all the participating entities of the system. It is a sealed, cryptographically verified, and immutable record of the exchanges that at any point occurred among the members. Considering the remarkable properties of blockchain which combine changelessness, acceptance, decentralization, and straightforwardness the blockchain promises to provide protection and safety to the information. Therefore, the blockchain will aid varied developing applications including keen urban areas like sanitation, agriculture, supply-chain, industries, banking, transportation and the Internet of Vehicles [9-11]. A typical Smart City is an urban framework where several smart prerequisites exist with every service, governance, policies and other information exchanges like a practical administration model of automated traffic management and open vehicle. It is a setting wherein residents can work remotely in almost all chores of events with the utilization of smart arrangements of energy, use of suitable innovation for saving energy and to minimize the ecological effect. The "smart city" idea includes a few parameters that interface with one another, which makes the quest for a precise definition a complex task. As per one definition it is defined as "The savvy use of innovation so as to gather, analyse, procedure, and execute a lot of valuable information legitimately from the previously working urban areas" [9]. The smart city ecosystem can be thought as an umbrella term where several modern day enabling technologies like ICT, blockchain, AI, Deep learning, machine learning , IoT, cloud/edge computing etc are integrated and works in synchronization to provide solutions to the users. These solutions include automation of essential services, governance, smart transportation, smart agriculture and smart habitat. It involves novel energy efficient frameworks and models, smart grids etc [5], [12].

## 1.1. Manuscript Organization

The manuscript is divided into 6 sections. Section 2 provides the systematic literature review of the recent researcher works. Section 3 provides security threats and issues associated with the implementation of blockchain technologies. Section 4 highlights the inherent challenges of blockchain based smart city ecosystem. Section 5 reviews the existing security proposals for blockchain based smart city adoptions. Section 6 summarizes the manuscript and provides the conclusion. It further highlights the future research directions of blockchain based smart city adoptions.

## 1.2. Why Blockchain?

There are several unprecedented properties of the blockchain technology that makes it an appropriate solution for several critical applications domains like healthcare, transportations, agriculture, education and forecasting etc. Some of these properties are given here in figure 1 [13-14].

- Transparency: All blockchain trades are crystal clear, which implies an aggregate, obvious and constant record of any activity that exists.
- Immutable and Non Repudiation: This means that with blockchain there is no danger of illegitimate extraction and a blockchain agreement can't be dropped by the sender when it sent and deleted.
- Speed: Affirmations and transactions of blockchain based trades can happen much faster as compared to legacy methods.
- Secure: Inherent security mechanism of blockchain makes it an appropriate solution of performing sensitive transactions in a distributed manner.
- Scalability and Extensibility: The typical architecture of blockchain makes it flexible to extend and scale the existing infrastructure without much difficulty and overhead.
- Distributed and Decentralized: At the core, the blockchain technology is a "distributed ledger" and follows a peer-to -peer architecture and thus eliminating the limitations of typical centralized systems.

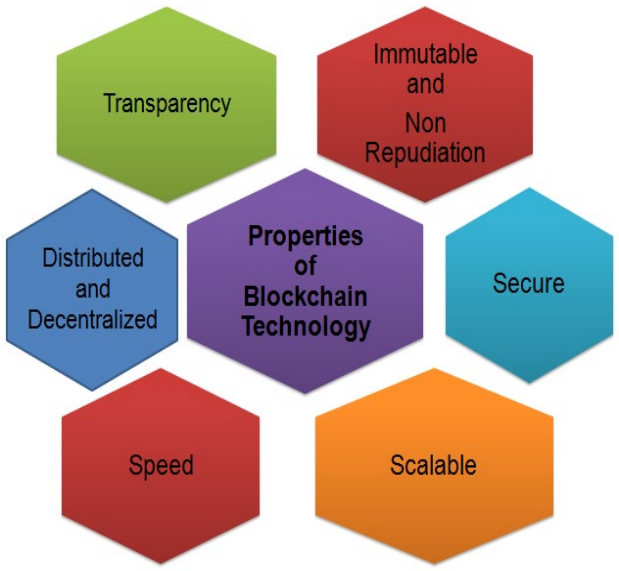


**Figure 1.** Properties of Blockchain

## 2. Related Works

This section provides some of the recent development in the field of blockchain based smart cities proposals.
The authors in [15] proposed a blockchain based mechanism for securely storing data from IoT based sensors placed at multiple surroundings of the point of interest. They proposed to use Ethereum blockchain and SCRUM technology for the implementation of their proposal. The authors in [16] provided a review of the existing literature on importance digital identity of the users and methods available for their protections. They primarily highlighted the blockchain based methods and discussed the issues and challenges associated with such systems. The authors in [17] proposed a blockchain based approach for securing and providing a transparent lottery management system. The specifically used "smart contracts and cryptograph blockchain model" in their proposal. In [18] the authors put forth a new "future living framework" based on blockchain technology to provide services and unique codes to the users. The applications domains and challenges associated in integration blockchain with smart living ecosystem is addressed. The authors in [19] proposed to apply blockchain and smart contracts in the real state sector. Their proposal provides a secure and privacy preserved means for the financial transactions between landlords and tenants. In [20] the authors proposed to decouple the transaction data from the blockchain headers in order to enhance the transaction speed. The supported the proposal with empirical evaluation using network emulator. The results show the effectiveness of their proposal as compared to existing solutions. The authors in [21] provided the extensive review of researches on blockchain technology applied in smart cities. A comprehensive roadmap of the research was provided including motivation, background and need of the research conducted. Finally some future aspects and scope were discussed. In [22], the authors provided privacy persevered SVM based data training scheme using blockchain technology. Their proposal eliminated the use of third party dependency and thus securing the data in transit. The authors in [23] proposed a lighter and novel security protocol using ethereum blockchain. The primary aim is to minimize the overhead of the network and provide better security. The source of the data origin can be authenticated using ethereum building blocks. The authors in [24] provided a mechanism for smart and sustainable economic services using fog computing and blockchain based storage. Their proposed framework was supported with implementation details and results showing the effectiveness of the proposal. The authors in [25] provided a blockchain based mechanism called as "BIS" for insurance industries in the smart cities. It uses POC based contract and data sharing mechanism. The primary aim of the proposal was to minimize the delay in processing of request and services of the insurance industries. In [26] the authors proposed a mechanism for sharing the data in a "secured and privacy preserved manner". The main idea of the proposal is to distribute the blockchain network into multiple channels with each channel having a specific capacity and constrained to process only specific type of data and thus the overall network congestion is distributed to gain performance enhancement.

## 3. Security Threats & Issues of Blockchain Technology

One most appealing highlights of blockchain innovation is its security component, which depends on distributed consensus and a public ledger. This doesn't imply that it can oppose any sorts of extortion and hacking. In recent years, the blockchain technology has been put to test and several security vulnerabilities were found as shown in figure 2 [27-31].

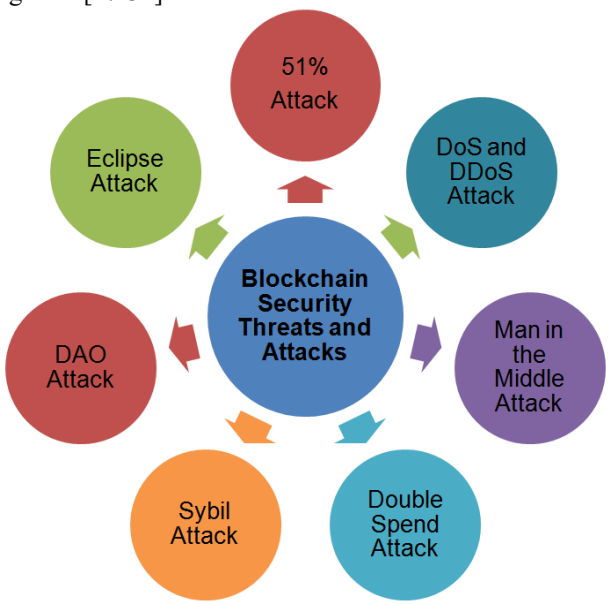


**Figure 2.** Security Threats and Attacks on Blockchain

- 51% Attack: They are the most regular assault on the blockchain based systems. They basically targets smaller networks and occurs when the hackers controls 51% of the nodes in the whole network.
- Double Spend Attack: The "double spend attack" comprises of spending a similar coin twice.
- DoS and DDoS Attack: The assaults like "Denial of Service (DoS) or Distributed DoS" aim at flooding the network with fake requests such that the legitimate requests cannot be serviced by the network.

- Man-in-the-Middle Attack: The aim of this attack is to hack the communication between two users and illegitimately relay spurious communication by altering the original contents.
- Eclipse Attack: These attacks occur when the hackers tricks the nodes to chose the peer from the malicious nodes instead of legitimate nodes.
- DAO Attack: Categorized as one of the most devastating attacks in history of blockchain. Here a bug was identified in the code and was used to illegitimately withdraw the money from users account.
- Sybil Attack: Here the attackers flood the network with malicious nodes in order to trick the legitimate nodes to choose peers. This attack is generally used to target a group of user or the complete network as a whole.

As discussed in [2], other significant dangers to smart urban communities are:

- Threats to availability: This includes issues like unapproved and illegitimate asset retention.
- Threats to integrity: This incorporate unapproved and illegitimate information alteration
- Threats to confidentiality: It incorporates disclosure of sensitive data or impersonation.
- Threats to authenticity: It includes unapproved access to assets and sensitive data.
- Accountability threats: This incorporate forswearing of transmission or gathering of a message by the related substance

.

Moreover, innovation advances with time and consequently new vulnerabilities and security threats are discovered. These newly discovered bugs and threats can further compromise open blockchains initiatives in near future.

The non-appearance of a focal position, the non-existent stamping element, and subsequently the complete lack of control is an alluring and simultaneously hazardous quirk. Numerous “private” and “permissioned” blockchain applications have been developed as of late to counter this.

## 4. Challenges of Blockchain Based Smart City

Compatibility barriers are the primary potential safety concern that still needs to be addressed. There are several other safety concerns that should still be handled [32], [45-49]. Some of them are given below:

- The absence of innovations that will have the option to process huge volumes of information. The 5V model of big data constitutes a core element of a smart city model.
- Use of IoT would entail a huge concentration of administrations, software, and associated hubs. Each one of these components may uncover the heterogeneity of their usefulness that will inevitably uncover vulnerabilities in security.
- One of the biggest problems is the lack of predefined standard benchmarks. The way things are, there is no general security consensus that will be utilized as a rule on the most proficient method to capture, handle, process, and appropriate information.

As expressed in [33-36], another set of difficulties include:

- Relying on a centralized cloud computing frameworks unavoidably acquires dubious latencies and dependencies on third party services.
- Although the Fog/Edge processing-based framework can meet the prerequisites raised by delay-sensitive, crucial applications but there is an acute shortage of skilled workforce [34-36].

New difficulties are additionally presented by the disseminated, cross-space highlights, for example, versatility, heterogeneity, and interoperability. A portion of the difficulties in a blockchain based smart city ecosystem addressed in [37] are:

- Structural versatility: Structural adaptability should be addressed when planning the engineering for an integrated smart city. This property allows the construction of a structure when appropriate without requiring critical system design changes.
- Network data transmission imperatives: Concentrated engineering-based arrangements are not fitting because of system transfer speed restrictions.
- Protection and security: The smart city system gives rise to numerous security and protection concerns and difficulties due to the exponential rise in the number of gadgets connected within the smart city ecosystem.
- Single point of failures: Smart city ecosystem can have a large number of single-point-of- failures as a result of heterogeneous nature of participating devices and data models.

## 5. Different Proposed Security Frameworks

Smart city ecosystem is centred around suitability, computerized administrations, instalments, and conditions, however, it ought to be improved. Various attempts in this area are the development of “Open Web Application Security Project (OWASP)”, “Computer Emergency Response Teams (CERT)” , “G-Cloud” for “Cloud Computer Service Provider (CCSP)” etc. [38-40]. Security perspectives are talked about by Biswas et. al [2], Simona Ibba et. al [15], Theodorou et. al [32] and P.K. Sharma [37] in their work. These works have been thought about as it examines the need for a particular security structure. one such system is made out of four layers [2], [15]:

- Physical Layer: Smart city devices (e.g. "Nest thermostat" and "Acer Fitbit") are fitted with sensors and actuators that capture and forwards the information to the upper layers; These devices are helpless against security attacks and vulnerabilities due to lack of encryption and access control instruments [41].
- Communication Layer: The blockchain mechanism should be coordinated with this layer to provide security and protection to the transmitted information. Mechanisms like BitTorrent can be utilized for distributed correspondence through Ethereum for providing smart agreement functionalities.
- Database Layer: A "distributed ledger" in the blockchain is a kind of "decentralized database" which stores recording in steady progression. There are two distinct kinds of dispersed records practically speaking:
  i) permission-less and ii) permissioned. It is prescribed to utilize private records to guarantee versatility, execution, and security for constant applications.
- Interface Layer: Each layer contains a variety of apps that work together to settle on mutually agreed positive choices.

In [32], a specialized methodology on how the innovation fills in rather than the conventional method for transferring and handling information has been introduced. Despite the fact that the highlights that make a smart city secure are various, they centred uniquely around those regions that are regarded as critical, for example, information management and circulation, correspondence, protection, verifying outsiders, savvy agreements and conventions (method for dealing with information). In [37], a novel hybrid design by utilizing the quality of developing "Software Defined Networking" and "blockchain advancements" has been discussed to address the difficulties of dynamic network management and security concerns. To guarantee security and protection in the model examined, Argon2 based Proof-of-Work plot is presented. The model was re-enacted over a private Ethereum blockchain network. The consequence of the assessment shows the adequacy of the proposed model. To take care of the issue of the sensors information storage and the management was discussed in [32]. Simona Ibba et. al [15] proposed to build up a product dependent on blockchain and to apply the SCRUM philosophy as a result of its capacities of being adaptable, versatile and iterative system. Like in [37], they have utilized the Ethereum stage to record estimations landing from the IoT system of sensors.

Lately, the "smart grid decentralization" has become a subject of research expecting to give an option in contrast to focal substances. In [42], the authors proposed a blockchain-based engineering for disseminating the management, control, and approval of interest reaction (DR) programs in low/medium voltage smart grids with a perspective on guaranteeing high unwavering quality and decentralized activity by actualizing identifiable and sealed vitality adaptability exchanges. The network has been demonstrated as a chart of peer nodes that can facilitate through a "blockchain-based framework" to aid "decentralized-energy" demand. A blockchain appropriated record is built and oversaw at the core framework level. The proposed approach was approved using a model actualized in an Ethereum stage [15], [37] using appropriate utilization mechanism and creating hints of a few structures from writing informational collections. The outcomes have demonstrated that blockchain-based conveyed request side administration can be utilized for coordinating critical request and creation at shrewd lattice level. The adoption of the "blockchain" will convert the "smart grid" into a "popularity-based network" that never again depends on a central position rather it can take any choice through smart contract rules dynamically. Dheeraj Nagothu et. al [33] presented a new secure smart reconnaissance framework dependent on "micro-services design" and "blockchain innovation" which is inherently dependent on various levelled edge-haze distributed computing worldview. The ability of consistent improvement and ceaseless conveyance permit a progressively adaptable and versatile reconnaissance framework. To verify the information traded among micro-services, the blockchain enables the administrator to track the information and keep away from information altering. "Smart contracts" have computerized the working of blockchain information and it gives the most significant level of information encryption for proficient and secure correspondence.

The rising ad hoc system for vehicles using the smart city was inspected in [43] and presented a blockchain-dependent circulated concept for the vehicle system to address difficulties. A "Block-VN model", dependent on blockchain arrangements for enabling smart transportation allows an increasingly productive and powerful improvement of the disseminated system of huge-scale vehicles. The Block-VN model enables the participating entities (vehicles) to recognize and share their assets in order to create an IoV system.

## 6. Conclusion

Blockchain is a vital component for providing a transparent, secured and privacy preserved information storage and circulation. When it is combined with other enabling technologies it can provide an unprecedented mechanism of information exchange across the network. In addition, different lightweight cryptographic natives ought to be added to increase the degrees of execution of several interconnected nodes. The expense of implementing the execution of a protected smart city ecosystem could be divided into several sub tasks. Sklavos and Souras [44] provided a model of the classifications of expenses that ought to be considered. Although there are several state-of-the-art solutions for realizing the smart city concept, yet a lot of scope is there

for improvement in every aspect of the smart city model. The security of the system and the participating entities being the primary concern that needs to be addressed more holistically. The complex nature of the underlying infrastructural requirements is causing hindrances in the realization of a smart city in true sense. The cost involved and the scarcity of the skilled manpower are the other limiting factors to be considered. Finally, it can be concluded that blockchain is an appropriate technology that can be used for providing a secured and privacy preserved mechanism of information exchange across the smart city ecosystem.

## References


[1] Merry H. Population increase and the smart city. 2018 [Available online] https://www. ibm. com/blogs/internet-of-things/increased-populationsmart-city. Accessed date 12 December 2019.

[2] Biswas K, Muthukkumarasamy V. Securing smart cities using blockchain technology. In 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS) 2016 Dec 12 (pp. 1392-1393). IEEE.

[3] Madaan N, Ahad MA, Sastry SM. Data integration in IoT ecosystem: Information linkage as a privacy threat. Computer law & security review. 2018 Feb 1;34(1):125-33.

[4] Ahad MA, Tripathi G, Zafar S, Doja F. IoT Data Management—Security Aspects of Information Linkage in IoT Systems. In Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm 2020 (pp. 439-464). Springer, Cham.

[5] Panetta K. Smart Cities Look to the Future. 2018. [Available online] https://www. gartner. com/smarterwithgartner/smart-cities-look-to-the-future. Accessed date. 06 November 2019.

[6] J. D. Lovelock, et al. "Forecast: Blockchain Business Value", Worldwide, 2017-2030, 2018

[7] N. M. Rosario, The Emerging Blockchain Patent Landscape, 2017

[8] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things. Ieee Access. 2016 May 10;4:2292-303.

[9] Mohanty SP, Choppali U, Kougianos E. Everything you wanted to know about smart cities: The internet of things is the backbone. IEEE Consumer Electronics Magazine. 2016 Aug 10;5(3):60-70.

[10] Puthal D, Mir ZH, Filali F, Menouar H. Cross-layer architecture for congestion control in Vehicular Ad-hoc Networks. In 2013 International Conference on Connected Vehicles and Expo (ICCVE) 2013 Dec 2 (pp. 887-892). IEEE.

[11] Pramanik MI, Lau RY, Demirkan H, Azad MA. Smart health: Big data enabled health paradigm within smart cities. Expert Systems with Applications. 2017 Nov 30;87:370-83.

[12] Ahad MA, Biswas R. Request-based, secured and energy-efficient (RBSEE) architecture for handling IoT big data. Journal of Information Science. 2019 Apr;45(2):227-38.

[13] Li X, Jiang P, Chen T, Luo X, Wen Q. A survey on the security of blockchain systems. Future Generation Computer Systems. 2017 Aug 23.

[14] de Leon DC, Stalick AQ, Jillepalli AA, Haney MA, Sheldon FT. Blockchain: properties and misconceptions. Asia Pacific Journal of Innovation and Entrepreneurship. 2017 Dec 4.

[15] Ibba S, Pinna A, Seu M, Pani FE. CitySense: blockchain-oriented smart cities. In Proceedings of the XP2017 Scientific Workshops 2017 May 22 (pp. 1-5).

[16] Rivera R, Robledo JG, Larios VM, Avalos JM. How digital identity on blockchain can contribute in a smart city environment. In2017 International smart cities conference (ISC2) 2017 Sep 14 (pp. 1-4). IEEE.

[17] Liao DY, Wang X. Design of a blockchain-based lottery system for smart cities applications. In2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC) 2017 Oct 15 (pp. 275-282). IEEE.

[18] Marsal-Llacuna ML. Future living framework: Is blockchain the next enabling network?. Technological Forecasting and Social Change. 2018 Mar 1;128:226-34.

[19] Karamitsos I, Papadaki M, Al Barghuthi NB. Design of the blockchain smart contract: A use case for real estate. Journal of Information Security. 2018 Jun 28;9(3):177-90.

[20] Michelin RA, Dorri A, Steger M, Lunardi RC, Kanhere SS, Jurdak R, Zorzo AF. SpeedyChain: A framework for decoupling data from blockchain for smart cities. InProceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services 2018 Nov 5 (pp. 145-154).

[21] Xie J, Tang H, Huang T, Yu FR, Xie R, Liu J, Liu Y. A survey of blockchain technology applied to smart cities: Research issues and challenges. IEEE Communications Surveys & Tutorials. 2019 Feb 15;21(3):2794-830.

[22] Shen M, Tang X, Zhu L, Du X, Guizani M. Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. IEEE Internet of Things Journal. 2019 Feb 26;6(5):7702-12.

[23] Reilly E, Maloney M, Siegel M, Falco G. A smart city iot integrity-first communication protocol via an ethereum blockchain light client. InProceedings of the International Workshop on Software Engineering Research and Practices for the Internet of Things (SERP4IoT 2019), Marrakech, Morocco 2019 Apr (pp. 15-19).

[24] Rahman MA, Rashid MM, Hossain MS, Hassanain E, Alhamid MF, Guizani M. Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city. IEEE Access. 2019 Jan 30;7:18611-21.

[25] Sharifinejad M, Dorri A, Rezazadeh J. BIS-A Blockchain-based Solution for the Insurance Industry in Smart Cities. arXiv preprint arXiv:2001.05273. 2020 Jan 15.

[26] Makhdoom I, Zhou I, Abolhasan M, Lipman J, Ni W. PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Computers & Security. 2020 Jan 1;88:101653.

[27] Eyal I, Sirer EG. Majority is not enough: Bitcoin mining is vulnerable. In International conference on financial cryptography and data security 2014 Mar 3 (pp. 436-454). Springer, Berlin, Heidelberg.

[28] Abilash Soundararajan, 10 Blockchain and New Age Security Attacks You Should Know, 2019. Url: https://blogs.arubanetworks.com/solutions/10-blockchain-and-new-age-security-attacks-you-should-know/. Accessed on 12 December 2019.

[29] Efanov D, Roschin P. The all-pervasiveness of the blockchain technology. Procedia Computer Science. 2018 Jan 1;123:116-21.
[30] Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems. 2018 May 1;82:395-411.
[31] Karame G, Androulaki E, Capkun S. Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin. IACR Cryptology ePrint Archive. 2012 Oct 16;2012(248).
[32] Theodorou S, Sklavos N. Blockchain-Based Security and Privacy in Smart Cities. In Smart Cities Cybersecurity and Privacy 2019 Jan 1 (pp. 21-37). Elsevier.
[33] Nagothu D, Xu R, Nikouei SY, Chen Y. A microservice-enabled architecture for smart surveillance using blockchain technology. In 2018 IEEE International Smart Cities Conference (ISC2) 2018 Sep 16 (pp. 1-4). IEEE.
[34] Nikouei SY, Chen Y, Song S, Xu R, Choi BY, Faughnan TR. Real-time human detection as an edge service enabled by a lightweight cnn. In2018 IEEE International Conference on Edge Computing (EDGE) 2018 Jul 2 (pp. 125-129). IEEE.
[35] Chen N, Chen Y, Blasch E, Ling H, You Y, Ye X. Enabling smart urban surveillance at the edge. In2017 IEEE International Conference on Smart Cloud (SmartCloud) 2017 Nov 3 (pp. 109-119). IEEE.
[36] Xu R, Nikouei SY, Chen Y, Polunchenko A, Song S, Deng C, Faughnan TR. Real-time human objects tracking for smart surveillance at the edge. In2018 IEEE International Conference on Communications (ICC) 2018 May 20 (pp. 1-6). IEEE.
[37] Sharma PK, Park JH. Blockchain based hybrid network architecture for the smart city. Future Generation Computer Systems. 2018 Sep 1;86:650-5.
[38] OWASP T. Application Security Risks 2017. Available (accessed November 16, 2019): https://www. owasp. org/index. php/Top_10-2017_Top_10. 10.
[39] Claycomb WR, Nicoll A. Insider threats to cloud computing: Directions for new research challenges. In2012 IEEE 36th Annual Computer Software and Applications Conference 2012 Jul 16 (pp. 387-394). IEEE.
[40] HM Government, Government cloud strategy, 1–24, 2011
[41] M. Seliger," Test: Fitness wristbands reveal data", Test AVTEST GmbH, Klewitzstr, Germany, 1–7, Jun. 2015
[42] Pop C, Cioara T, Antal M, Anghel I, Salomie I, Bertoncini M. Blockchain based decentralized management of demand response programs in smart energy grids. Sensors. 2018 Jan;18(1):162.
[43] Sharma PK, Moon SY, Park JH. Block-VN: A distributed Blockchain based vehicular network architecture in smart city. Journal of Information Processing Systems. 2017 Feb 1;13(1).
[44] Sklavos N, Souras P. Economic Models & Approaches in Information Security for Computer Networks. IJ Network Security. 2006 Jan 1;2(1):14-20.
[45] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Manubot; 2019 Nov 20.
[46] Lazaroiu C, Roscia M. Smart district through iot and blockchain. In2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA) 2017 Nov 5 (pp. 454-461). IEEE.
[47] Reyna A, Martín C, Chen J, Soler E, Díaz M. On blockchain and its integration with IoT. Challenges and opportunities. Future generation computer systems. 2018 Nov 1;88:173-90.
[48] Puthal D, Malik N, Mohanty SP, Kougianos E, Yang C. The blockchain as a decentralized security framework [future directions]. IEEE Consumer Electronics Magazine. 2018 Feb 8;7(2):18-21.
[49] Sun J, Yan J, Zhang KZ. Blockchain-based sharing services: What blockchain technology can contribute to smart cities. Financial Innovation. 2016 Dec;2(1):1-9.